IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF PENNSYLVANIA

DRESSER-RAND COMPANY,	:	
Plaintiff,	:	
	:	CIVIL ACTION
v.	:	
	:	NO. 10-2031
G. CURTIS JONES, JEFFREY KING,	:	
ALBERT E. WADSWORTH, IV, and	:	
GLOBAL POWER SPECIALIST, INC.	:	
Defendants.	:	

July 23, 2013 **Anita B. Brody, J.**

MEMORANDUM

Plaintiff Dresser-Rand Company ("Dresser-Rand") brings a variety of claims against G. Curtis Jones, Jeffrey King, Albert E. Wadsworth, IV, and Global Power Specialist, Inc. ("Global Power"), including a claim for violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("the CFAA").[1] I exercise jurisdiction pursuant to 28 U.S.C. § 1331 and 28 U.S.C. § 1332. Defendants filed a partial motion for summary judgment against Plaintiff on the CFAA claims. *See* ECF No.72. For the reasons stated below I will grant Defendants' partial motion for summary judgment.

[1] Plaintiff brings six counts against all Defendants: Misappropriation of Trade Secrets, 12 Pa.C.S.A. § 5302, violation of the CFAA, conversion, unjust enrichment, unfair competition, and tortious interference with prospective economic damage. Plaintiff brings two counts against Jones and King: breach of fiduciary duty and breach of duty of loyalty, one count against Wadsworth for aiding and abetting breach of fiduciary duty, one count against Jones for breach of contract, and one count against Jones, King, and Wadsworth for conspiracy. Defendants' motion for partial summary judgment only concerns the CFAA claim.

I. BACKGROUND[2]

G. Curtis Jones and Jeffrey King worked as managers for the Dresser-Rand Company, a $2 billion corporation that provides technology, product and services used for developing energy and natural resources. Dresser-Rand's business includes manufacturing industrial equipment and field services operations to maintain and service industrial equipment for Dresser-Rand clients who own power plants, industrial plants and refineries. Jones resigned from Dresser-Rand on February 9, 2010 from his position as Regional Field Services Manager. King resigned from Dresser-Rand on February 26, 2010 from his position as Project Manager.

On January 20, 2010, prior to the resignations of Jones and King, Albert Wadsworth incorporated Global Power Specialist, Inc. and became Global Power's president. Jones and King became Global Power's two employees. Global Power performs field services work to fix gas turbines. Jones and King had Global Power cellphones and e-mail addresses and performed work to benefit Global Power before they resigned from Dresser-Rand. Before Jones and King left Dresser-Rand, they downloaded Dresser-Rand documents to external hard drives and flash drives. Dresser-Rand's forensic computer expert found that on multiple occasions from December 2009 through February 2010 Jones and King downloaded Dresser-Rand files onto at least five external devices. They downloaded the files days before they each resigned.[3] On

[2] For purposes of summary judgment, "the nonmoving party's evidence is to be believed, and all justifiable inferences are to be drawn in [that party's] favor." *Hunt v. Cromartie,* 526 U.S. 541, 552, (1999) (alteration in original) (internal quotation marks omitted).

[3] Jones and King claim that they downloaded the files because they were told by their supervisors to back up the data on their Dresser-Rand laptops onto external hard drives. King kept personal files, family photographs, and music on his Dresser-Rand laptop. He claims that he transferred all of the contents of his Dresser-Rand computer to his Global Power computer because he did not know how to use the hard drive to select documents to back up. He admitted that he did not download those documents for the benefit of Dresser-Rand, but to preserve his

February 25, 2010, King e-mailed to Wadsworth, “I shit canned everything on my computer since I have to turn it in tomorrow.” Pl. Ex. J.

Dresser-Rand’s computer expert found that thousands of Dresser-Rand’s files were transferred from the external devices to Global Power’s computers. Defendants accessed some of these files from Global Power computers after they left Dresser-Rand. Wadsworth received e-mails from Jones and King sent from their Dresser-Rand computers containing Dresser-Rand business information. He reviewed and edited some of these documents.

Dresser-Rand’s Director of Services for the Mid-Atlantic Region Glenn “Chip” Jones stated that he had “no reason to believe that [Jones and King] accessed information other than what they had authorized access to do through their Dresser-Rand user name and password.” Def. Ex. A 191:23-25, 192:2-5. Chip Jones testified as an individual. Pl. Response at 5 n.5.

Dresser-Rand has several policies that govern employee use of Dresser-Rand resources and information. These policies include a Code of Conduct that covers conflicts of interest, competition and fair dealing, confidentiality, privacy, protection and proper use of company assets, and other topics. Pl. Ex. B. Dresser-Rand’s Internet Access and Usage Policy provides that unauthorized use of the internet includes “[s]ending, receiving or posting without authorization company-sensitive or privileged information . . .”. Ex. G. Dresser-Rand’s Acceptable Use Policy states that “Any unauthorized use, disclosure or transmission of [protected] information or content is prohibited. Users are required to comply with all applicable laws, agreements and Company policies before placing any information of a proprietary, confidential, or trade secret nature into Dresser-Rand’s computers.” Pl. Ex. H at 2. Each time

work history. Dresser-Rand’s computer expert found that the manner in which the downloads were made to the external devices was not consistent with “backing up” a hard drive.

Dresser-Rand employees log on to a company computer, they must acknowledge and accepts the company's "Legal Notice and Acceptable Use Statement":

> This is a Dresser-Rand (D-R) System. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided solely for the purpose of authorized D-R business use. Any use or activity that jeopardizes the integrity of the equipment, violates any Company policy, or is not in the best interests of the Company, is strictly prohibited. There is no confidentiality or privilege when used for personal rather than Company or work related communications . . . All information entered into this computer system is D-R property and may constitute D-R confidential information. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use.

Pl. Ex. I.

Defendants filed a partial motion for summary judgment on November 9, 2010 concerning the CFAA claims only. On December 16, 2010 the case was placed in suspense pending conclusion of a related criminal investigation. On April 16, 2013, Plaintiff notified the Court that the criminal investigation concluded and that Defendants would not be charged.

II. LEGAL STANDARD

Summary judgment will be granted "if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). A fact is "material" if it "might affect the outcome of the suit under the governing law . . . ." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). A factual dispute is "genuine" if the evidence would permit a reasonable jury to return a verdict for the nonmoving party. *Id.*

The moving party bears the initial burden of demonstrating that there is no genuine issue of material fact. *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986). The nonmoving party must then "make a showing sufficient to establish the existence of [every] element essential to that party's case, and on which that party will bear the burden of proof at trial." *Id.* at 322. However, the nonmoving party may not "rely merely upon bare assertions, conclusory allegations or suspicions" to support its claims. *Fireman's Ins. Co. of Newark, N.J. v. DuFresne*, 676 F.2d 965, 969 (3d Cir. 1982).

In essence, the inquiry at summary judgment is "whether the evidence presents a sufficient disagreement to require submission to a jury or whether it is so one-sided that one party must prevail as a matter of law." *Anderson*, 477 U.S. at 251-52.

III. DISCUSSION

The Computer Fraud and Abuse Act prohibits seven types of computer crimes mainly involving accessing computers without authorization or in excess of authorization, and then obtaining information or damaging computer data. 18 U.S.C. § 1030(a). The statute, enacted by Congress in 1984, was originally exclusively a criminal statute. Since then the statute has been amended several times, including in 1994, when Congress amended the act to add a civil provision. Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322, § 290001(d), 108 Stat. 1796 (codified at 18 U.S.C. § 1030(g)). A violation of the statute exposes one to both civil and criminal liability.[4]

Legislative history reveals that "[t]he general purpose of the CFAA was to create a cause of action against computer hackers (e.g., electronic trespassers)." *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008) (internal quotation marks omitted); *accord US Bioservices Corp. v. Lugo*, 595 F. Supp. 2d 1189, 1193 (D. Kan. 2009) ("The CFAA was

[4] A civil action can be brought if the conduct involves at least one of several factors, such as incurring "a loss aggregating at least $5,000 in value," as alleged here. *See* 18 U.S.C. §§ 1030(c)(4)(A)(i)(I)-(V), 1030(g); Compl. ¶ 141.

intended as a criminal statute focused on 'hackers' who trespass into computers . . . ."). For example, the 1984 House Committee Report noted that under § 1030 "the conduct prohibited is analogous to that of 'breaking and entering' rather than using a computer (similar to the use of a gun) in committing the offense." H.R. Rep. No. 98-894, at 20 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3706. Additionally, other Congressional reports have characterized the CFAA as a statute prohibiting computer trespass. Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1618, 1668 n.90 (2003) (citing S. Rep. No. 104-357, at 11 (1996); S. Rep. No. 99-432, at 9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2487). An analogy to burglary provides clarity to the limitations of the CFAA: "If a person is invited into someone's home and steals jewelry while inside, the person has committed a crime—but not burglary—because he has not broken into the home. The fact that the person committed a crime while inside the home does not change the fact that he was given permission to enter." Thomas E. Booms, *Hacking into Federal Court: Employee "Authorization" Under the Computer Fraud and Abuse Act*, 13 VAND. J. ENT. & TECH. L. 543, 571 (2011).

The statutory provision relevant to this case provides that

> **(a)** Whoever . . .
>
> **(4)** knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;
>
> . . . shall be punished as provided in subsection (c) of this section.

18 U.S.C. § 1030(a)(4).

"Access" is not defined. "Exceeds authorized access" is defined as: "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

Dresser-Rand argues that all of the Defendants—King, Jones, Wadsworth and Global Power violated this section of the CFAA. Dresser-Rand's arguments supporting this allegation are summarized as follows:

- King and Jones exceeded their authorized access to Dresser-Rand's computers by downloading files to flash drives and external hard drives for the benefit of Global Power and in violation of Dresser Rand policy;

- King exceeded his authorized access when he "shit-canned" his Dresser-Rand laptop;

- Wadsworth and Global Power violated the CFAA when King and Jones accessed their computers while acting as their agents; and

- Wadsworth violated the CFAA when he accessed and edited Dresser-Rand files sent to him by Jones and King.

To demonstrate that the Defendants violated section 1030(a)(4) of the CFAA, Dresser-Rand must prove that "(1) [the] defendant had accessed a 'protected computer;' (2) has done so without authorization or by exceeding such authorization as was granted; (3) has done so 'knowingly' and with 'intent to defraud;' and (4) as a result has 'further[ed] the intended fraud and obtain[ed] anything of value.'" *See P.C. Yonkers, Inc. v. Celebrations The Party and Seasonal Superstore, LLC*, 428 F.3d 504, 508 (3d Cir. 2005).

A. CFAA Claims Against Wadsworth – "Access"

The Computer Fraud and Abuse Act governs activity that involves accessing or damaging computers.[5] Use of the computer is integral to the perpetration of a fraud under the CFAA, and not merely incidental. *Brett Senior & Assoc., P.C. v. Fitzgerald*, 2007 WL 2043377, at *4 (E.D. Pa. July 13, 2007). Whatever happens to the data subsequent to being taken from the computers subsequently is not encompassed in the purview of the CFAA. Dresser-Rand's CFAA claim against Wadsworth fails to meet the basic requirement of accessing a computer. Dresser-Rand does not allege in its Complaint that Wadsworth had any interaction with its computers, computer systems, or network—only that Wadsworth viewed and edited Dresser-Rand documents on his own computer that he received via e-mail attachments from Jones and King. Wadsworth may have accessed Dresser-Rand documents, but he never accessed Dresser-Rand computers, as required under the CFAA.

Dresser-Rand argues that Wadsworth is nonetheless implicated because Jones and King acted as his agents when they downloaded the files. Yet Dresser-Rand provides no legal basis in the CFAA or otherwise to justify imputing liability from the individuals who access a computer without authorization to others who may eventually benefit from their actions. Therefore Wadsworth cannot be held liable for a CFAA claim under these theories and I will grant Defendant's partial motion for summary judgment as to Wadsworth.

B. CFAA Claim against Jones and King – "Exceeding Authorized Access"

Unlike Wadsworth, King and Jones undisputedly accessed Dresser-Rand's computers. Whether King and Jones are liable under the CFAA turns on whether they "exceed[ed]

[5] The statute does not state that physically accessing a computer is required. Access could be accomplished remotely.

authorized access" when they downloaded files from their laptops. As noted above, although the CFAA does not define the word "access," it defines "exceeds authorized access," to mean, "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to so obtain or alter." 18 U.S.C. § 1030(e)(6). The term "authorization" is not further defined, leaving courts to wrestle with the breadth of its meaning as increasingly, employers have used a statute originally designed to punish hackers against disloyal employees. *See P.C. Yonkers, Inc. v. Celebrations The Party and Seasonal Superstore, LLC*, 428 F.3d 504, 510 (3d Cir. 2005). Determining an employee's authorization to company computer systems is further complicated by the proliferation of employer computer and internet use policies.

The circuit courts are split between what is cast as a broad versus a narrow interpretation of the term "without authorization." Under the narrow view, an employee given access to a work computer is authorized to access that computer regardless of his or her intent to misuse information and any policies that regulate the use of information. *See WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012); *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc); *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009). Under the broad view, if an employee has access to information on a work computer to perform his or her job, the employee may exceed his or her access misusing the information on the computer, either by severing the agency relationship through disloyal activity, or by violating employer policies and/or confidentiality agreements. *See U.S. v. John*, 597 F.3d 263 (5th Cir. 2010); *U.S. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010); *Int'l Airport Ctrs, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006); *Cultural Travel BV v. Explorica, Inc.*, 274 F. 3d 577 (1st Cir. 2001). Rather than using "broad" versus "narrow" labels, academics have helpfully divided the approaches of courts into three categories: agency-based authorization, code-based authorization, and contract-based authorization.[6] *See* Kerr, 78 N.Y.U. L. REV. at 1644-45; Katherine Mesenbring Field, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 821 (2009). The Third Circuit has not yet ruled as to whether it will adopt the broad or narrow interpretation of the statute.[7] Meanwhile, courts in the Eastern District of Pennsylvania have generally adopted the narrower interpretation.[8] I find the narrow

[6] Professor Orin Kerr defines code-based authorization as a situation where an owner codes the computer's software so that a user has a defined set of privileges on the computer, often limited through a unique password and account. "For a user to exceed privileges imposed by code, the user must somehow 'trick' the computer into giving the user greater privileges . . . Alternatively, a user can exploit a weakness in the code within a program to cause the program to malfunction in a way that grants the user greater privileges." *Id.* In contrast, in a contract-based authorization scenario, "an owner can condition use of the computer on a user's agreement to comply with certain rules," through Terms of Service, or Terms of Use, for example. *Id.* at 1645-46.

[7] Dresser-Rand attempts to argue that the Third Circuit has taken a stance in *P.C. Yonkers, Inc. v. Celebrations The Party and Seasonal Superstore LLC*, 428 F. 3d 504 (3d Cir. 2005). In *P.C. Yonkers*, the definition of "authorization" was not at issue. Rather, the Court affirmed a denial of a preliminary injunction because the plaintiff failed to show that defendants intended to defraud the plaintiff, an element required by the statute. *Id.* at 509. The plaintiff failed to show proof that any information was actually viewed or taken. *Id.* In dicta the Court stated that while most CFAA cases involve "classic" hacking activities, employers have increasingly used the CFAA's civil remedies to sue former employees who start new businesses that compete with their former employers. *Id.* at 510. Dresser-Rand improperly tries to invoke this statement to demonstrate that the Third Circuit would permit its CFAA claim to go forward. It is, however, merely a descriptive statement.

[8] *See Synthes, Inc. v. Emerge Medical, Inc.*, CIV.A. 11-1566, 2012 WL 4205476 (E.D. Pa. Sept. 19, 2012); *Grant Mfg. & Alloying, Inc. v. McIlvain*, CIV.A. 10-1029, 2011 WL 4467767 (E.D. Pa. Sept. 23, 2011) *aff'd*, 499 F. App'x 157 (3d Cir. 2012); *Clinton Plumbing and Heating of Trenton, Inc. v. Ciaccio, et. al.*, No. 09-2751, 2010 WL 4224473, (E.D. Pa. Oct. 22, 2010); *Integrated Waste Solutions, Inc. v. Goverdhanam*, CIV.A. 10-2155, 2010 WL 4910176 (E.D. Pa. Nov. 30, 2010); *Bro-Tech Corp. v. Thermax, Inc.*, 651 F. Supp. 2d 378 (E.D. Pa. 2009); *Brett Senior & Assoc., P.C. v. Fitzgerald*, 2007 WL 2043377 (E.D. Pa. July 13, 2007); *but see Hub Grp., Inc. v. Clancy*, CIV. A. 05-2046, 2006 WL 208684 (E.D. Pa. Jan. 25, 2006) (finding that for purposes of federal question jurisdiction, an employee exceeded the scope of his

interpretation adopted by the Ninth and Fourth Circuits to be true to the language of the statute and intentions of Congress.

Courts that adopt the narrow view base their reasoning on the plain language of the statute, dictionary definition of "authorization," and the rule of lenity. *See, e.g. WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012); *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc); *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009); *Bro-Tech Corp. v. Thermax, Inc.*, 651 F. Supp. 2d 378, 406-07 (E.D. Pa. 2009); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962 (D. Ariz. 2008); *Brett Senior & Assoc., P.C. v. Fitzgerald*, 2007 WL 2043377 (E.D. Pa. July 13, 2007). The Fourth Circuit goes through this analysis for a factual scenario very similar to this case. A WEC employee emailed downloaded confidential WEC documents to a personal computer prior to resigning from the company to work for one of its competitors. *WEC Carolina*, 687 F.3d at 202. The employee allegedly used the downloaded information to make a presentation on behalf of the competitor to a potential WEC customer, and won the projects for the competitor. *Id.* WEC had given the employee a laptop computer and authorized access to the company's intranet and servers. *Id.* WEC had policies "prohibiting the use of any confidential information and trade secrets unless authorized" and prohibiting the "download[ing] [of] confidential and proprietary information to a personal computer." *Id.* 206-07. Yet WEC alleged in its complaint that defendant "'had access to WEC's intranet and computer servers' and 'to numerous confidential and trade secret documents stored on these computer servers . . .'". *Id.* at 207.

authorization into his employer's database when he e-mailed confidential information to his wife, giving the employer the ability to plead a CFAA cause of action).

The Court began with examining the plain language of the statute. *Id.* at 203. It recites the Oxford English Dictionary definition for "authorization": "formal warrant, or sanction." *Id.* at 204 (citing *Oxford English Dictionary* (2d ed.1989; online version 2012)). Citing the Ninth Circuit's analysis in *LVRC Holdings LLC v. Brekka*,[9] the WEC Carolina Court concluded that "an employee is authorized to access a computer when his employer approves or sanctions his admission to that computer," an employee is "without authorization" when "he gains admission to a computer without approval," and an employee "exceeds authorized access" "when he has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access." *Id.* at 204 (citing *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009)). These definitions do not extend to improper use of information validly accessed. *Id.* at 204. Thus the WEC Carolina Court concluded that while defendants may have misappropriated information, they did not access a computer without authorization or exceed their authorized access. *Id.* at 207.

As for any ambiguity surrounding the term "without authorization," the Court noted that its interpretation would apply to both the civil and criminal parts of the statute, and therefore any ambiguity would be resolved in favor of lenity. *Id.* at 204. This rule ensures that we are shielded from unexpected criminal consequences of ambiguous statutes. *Id.* As a result, the Court was "unwilling to contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy." *Id.* at 207.

[9] The Ninth Circuit in *LVRC Holdings LLC v. Brekka* was the first circuit court to articulate the narrow view.

In an en banc opinion, the Ninth Circuit rejected the notion that that the CFAA encompasses corporate use restrictions. *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc).[10] In *Nosal,* employees of the Korn/Ferry company encountered a warning prior to logging in to the company's database stating, "This product is intended to be used by Korn/Ferry employees for work on Korn/Ferry business only." *Id.* at 856 n.1. Nonetheless, employees logged into the database and transferred confidential information to Nosal, a former employee who sought to create a competing business. *Id.* at 856. The Nosal Court held that if Korn/Ferry's policy established the nature of an employee's authorization, then the CFAA would allow employers "to manipulate their computer-use and personnel policies so as to turn these relationships into ones policed by the criminal law."[11] *Id.* at 860; See *also Brett Senior,* at *4 (concluding that a broad view of the CFAA would criminalize state-law breaches of contract). The Court was concerned with the ramifications of a broad interpretation of "without authorization," imagining a variety of seemingly innocuous scenarios that could lead to criminal or civil liability under the CFAA. For example, the Court opined that

> [b]asing criminal liability on violations of private computer use polices can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved. Employees who call family members from their work phones will become criminals if they send an email instead.

[10] For a history of the Nosal cases, see Kelsey T. Patterson, *Narrowing it Down to One Narrow View: Clarifying and Limiting the Computer Fraud and Abuse Act*, 7 CHAR. L. REV. 489, 509 n.126 (2013) (describing the lower court's pre and post *Brekka* decisions, the Ninth Circuit's initial ruling and reversal en banc).

[11] Professor Kerr elaborates further on this fear, arguing that courts should use the void-for-vagueness doctrine to narrow interpretation of "unauthorized access" under the CFAA in order to save the statute's constitutionality, because otherwise, its scope is too broad. Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561 (2010). He advocates for courts to clearly define "without authorization" to provide sufficient notice as to what activity is prohibited, and for courts to adopt a narrow interpretation to avoid discriminatory enforcement by the government. *Id.* at 1575.

> Employees can sneak in the sports section of the *New York Times* to read at work, but they'd better not visit ESPN.com. And sudoku enthusiasts should stick to the printed puzzles, because visiting www.dailysudoku.com from their work computers might give them more than enough time to hone their sudoku skills behind bars.

Nosal, 676 F.3d at 860. Going a step further, the Ninth Circuit expressed concern over terms of service agreements on internet sites that could change at a moment's notice, making previously legal behavior suddenly criminal through no act of Congress. *Id.* at 862. Employers could use the CFAA against employees in wrongful termination suits, or threaten to report employees to law enforcement. *Id.* at 860, n.6. As a result, the Ninth Circuit urged against applying the CFAA broadly based on employer use policies, fearing that it "would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute." *Id.* at 857. The Court concluded, "[i]f Congress wants to incorporate misappropriation liability into the CFAA, it must speak more clearly." *Id.* at 863. It clarified that "without authorization" applies to outside hackers, while "exceeds authorized access" applies to inside hackers. *Id.* at 858.

By adopting the narrow theory, the Ninth and Fourth Circuits rejected the Seventh Circuit's broad theory that authorization can be defined based on principles of agency law. *See WEC Carolina*, 687 F.3d at 206; *Nosal*, 676 F.3d at 862; *Brekka*, 581 F.3d at 1134. Under the Seventh Circuit's theory, when employees breach their duty of loyalty to their employers, they end their agency relationship with the company and are no longer authorized to access their work computers. *Citrin*, 440 F.3d at 420-21. Thus when an employee destroyed all of his files on his work laptop prior to quitting, the Seventh Circuit found that his "breach of his duty of loyalty terminated his agency relationship . . . and with it his authority to access the laptop, because the only basis of his authority had been that relationship." *Id.* at 419-20. The Ninth Circuit rejected the notion that a change in an employee's mental state from "loyal employee" to "disloyal competitor" will alter the employee's culpability under the CFAA based on the rule of lenity and plain meaning of the statute. *Brekka*, 581 F.3d at 1134. Such a rule bases authorization on the whim of the employee at the given moment he or she uses a computer. As the Fourth Circuit noted, if an employer could revoke authorization when an employee uses his or her access for a purpose contrary to the employer's interest, then an employee who checks a Facebook status or sports scores would instantly lose his or her agency, and therefore left without any authorization to access his or her employer's computer systems. *WEC Carolina*, 687 F.3d at 206. Furthermore, there is no mention of agency or loyalty in the CFAA, a statute that was designed to punish computer hackers.

No circuit courts have since evoked *Citrin*'s agency law theory. However, the First, Fifth and Eleventh Circuits have bowed to the whim of employer use policies and confidentiality agreements[12] to stretch the scope of the CFAA. The First Circuit found that an employee's access was limited by his intended use because he intended to directly compete with his employer's business in contravention of a confidentiality agreement he signed. *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581-82 (1st Cir. 2001). Similarly in *U.S. v. Rodriguez*, the Eleventh Circuit held that a Social Security Administration employee exceeded his authorized access when he accessed its databases for nonbusiness reasons in violation of the Administration's policies. *U.S. v. Rodriguez,* 628 F.3d 1258, 1260 (11th Cir. 2010). In *U.S. v. John*, the Fifth Circuit held that the defendant should have known that she was not authorized to access Citigroup's database to commit fraud. *U.S. v. John,* 597 F.3d 263, 271-72 (5th Cir. 2010).

[12] Academics call this "contract-based authorization." *See supra* note 6.

The Fifth Circuit focused on the fact that John used her access to the computer to commit a crime. Interestingly, the Court was reluctant to find "that violating a confidentiality agreement under circumstances such as those in [the First Circuit's case *Explorica*] would give rise to criminal culpability," though there is no reason why it could not be extended to the criminal context under the statute. *Id.*

These rulings wrap the intent of the employees and use of the information into the CFAA despite the fact that the statute narrowly governs access, not use. Courts in the Eastern District of Pennsylvania have rejected this notion. In *Brett Senior* Judge McLaughlin urged against looking at a defendant's motivation in accessing information because to do so would collapse the independent requirements of the statute into a single inquiry. *Brett Senior,* at *4. Subjective intent departs from the original view that the CFAA concerns what is "tantamount to trespass in a computer." *Clinton Plumbing and Heating of Trenton, Inc. v. Ciaccio, et. al.*, No. 09-2751, 2010 WL 4224473, at 5 (E.D. Pa. Oct. 22, 2010). The Ninth Circuit disapproved of the Eleventh, Fifth and Seventh Circuits' failure to consider the broad consequences of incorporating intent into the definition of "authorization," and to apply the rule of lenity. *Nosal,* 676 F.3d at 862-63. The statute simply does not support a broad interpretation of "authorization" based on employer use policies. Based on this conclusion, Jones' and King's conduct cannot be punishable under the CFAA.

First, the extent of Jones' and King's authorized access must be determined. Courts in the Eastern District of Pennsylvania have allowed CFAA claims to proceed when genuine issues of material fact exist as to the level of an employee's authorization. *Bro-Tech Corp.*, 651 F. Supp. at 407 (finding that "the quality or extent of a particular individual's authorization to access a computer is informed by the facts of the case.”). In *Bro-Tech* the court denied summary judgment because questions of fact existed regarding the nature and extent of the employees’ authorization to delete files they allegedly accessed. *Id.* at 407-08. Similarly, in *Feinberg v. Eckelmeyer*, the court declined to dismiss a CFAA claim where a question of fact existed as to when an employee ceased to be an owner of the company, which in turn defined his level of authorization to access the employer’s computers.[13] *Feinberg v. Eckelmeyer*, CIV.A. 2:09-cv-1536-WY, 2009 WL 4906376, at *9-10 (E.D. Pa. Dec. 16, 2009).

Jones and King accessed their work laptops and downloaded thousands of documents to external storage devices. If Jones and King were authorized to access their work laptops and to download files from them, they cannot be liable under the CFAA even if they subsequently misused those documents to compete against Dresser-Rand. The Plaintiff alleges that “Jones and King used the Company’s computers that *they were authorized to use* for legitimate Dresser-Rand business purposes to instead access and copy Dresser-Rand’s property, including its trade secrets and confidential information . . .”. Compl. ¶ 46 (emphasis added). King and Jones had user names and passwords to access the Dresser-Rand network and had access to their Dresser-Rand issued laptops and external hard drives. Chip Jones, Director of Services for the Mid-Atlantic Region, stated that he had “no reason to believe that [King and Jones] accessed information other than what they had authorized access to do through their Dresser-Rand user name and password.” Def. Ex. A, 191:23-25, 192:2-5. Dresser-Rand does not argue that there

[13] Curiously, Dresser-Rand describes *Feinberg v. Eckelmeyer* as rejecting the limited interpretation of the CFAA. Pl. Response at 12. *Feinberg* never adopted a broad view of the CFAA. Rather, the court found that the employee’s authorization to access the employer’s computers after a certain date was a question of fact that could not be resolved at the motion to dismiss phase. *Feinberg v. Eckelmeyer*, 2009 WL 4906376, at *9.

are limitations on employees' ability to copy documents to which they would otherwise have access to external storage devices like hard drives or flash drives. King and Jones' December 2009, January 2010 and February 2010 downloads all occurred while still employed by Dresser-Rand. Pl. Ex. A, Ex. 1-8. Based on this evidence, Jones and King were authorized to access their laptops and download files while they still were employed at Dresser-Rand.

Dresser-Rand argues that genuine issues of material fact exist regarding Defendants' authorization to access their computers. However, none of its asserted issues of material fact are actually material. Dresser-Rand arguing that Jones and King exceeded their authorized access when the violated Dresser-Rand's computer use policies and Code of Conduct. Dresser-Rand's corporate use restrictions, which resemble the policies in *Nosal* and *WEC*, cannot alter Jones' and King's authorized access. Dresser-Rand's "Legal Notice and Acceptable Use Statement" that appears before any employee can log on to the Dresser-Rand system is similar to the notice that appeared before accessing the database in *Nosal.* Like WEC's policies, Dresser-Rand's policies governed *use*, not *access*, strictly prohibiting "[a]ny use or activity that jeopardizes the integrity of the equipment, violates any Company policy, or is not in the best interests of the Company . . .". Pl. Ex. I. Therefore the policies are inapposite.[14]

[14] An open question remains as to whether a cleverly crafted employee use policy could define authorized access on the basis of the user's intent. The current "narrow' interpretation is still in actuality a narrow "contract-based authorization" theory. Contracts that govern use may not apply, but potentially, contracts that specifically govern access would circumvent this narrow interpretation of the CFAA. Patterson, 7 CHAR. L. REV. at 525-26. In a recent Northern District of California case, the court allowed CFAA claims to proceed because a former employer was verbally told he could only access his personal files on his old company's network, but no other work-related files. *Weingard v. Harland Fin. Solutions, Inc.*, No. C-11-3109 EMC, 2012 WL 2327660, at *3 (N. D. Cal. June 19, 2012). The court found that "although *Nosal* clearly precluded applying the CFAA to violating restriction on *use*, it did not preclude applying the CFAA to rules regarding *access*." *Id.* It rejected counsel's argument that "authorization" under

Dresser-Rand argues that disputed facts remain as to the frequency and purpose of the downloads by Jones and King from Dresser-Rand computers, specifically that the downloads were not routine "backups" of files onto an external hard drive. Because Jones and King were authorized to access files on the Dresser-Rand computers, and had no apparent download restrictions, the purpose of their downloads is irrelevant.

Dresser-Rand maintains that disputed facts exist concerning the Defendants' subsequent transfer of Dresser-Rand files to Global Power computers. Dresser-Rand's forensic computer expert noted that Jones and King accessed Dresser-Rand-originated files after they ceased their employment on Global Power computers. Because the CFAA is based on unauthorized computer access—not file access, the fact that files were accessed on Global Power computers is immaterial to the CFAA claim.

Because Jones and King had authorization to access their work computers, they did not hack into them when they downloaded the files. Their alleged misuse of the files may have remedies under other laws, but not under the CFAA. Therefore I will grant Defendants' partial motion for summary judgment as to Jones and King.

IV. CFAA Claim against King for Destroying Files

Dresser-Rand asserts that genuine dispute of material facts exists as to "[w]hat actions King took in "shit canning" his computer and thus destroying Dresser-Rand files." Pl. Response at 10. King wrote to Wadsworth that he "shit canned everything on my computer since I have to turn it in tomorrow." Pl. Ex. J. Dresser-Rand takes this e-mail to mean that King destroyed files. Other than this e-mail, there is no other evidence that King destroyed any files. In fact,

the CFAA is code-based, finding that *Nosal* did not go that far in narrowing the term. *Id.* Because Dresser-Rand's policies only govern use, I need not reach this issue.

Dresser-Rand's forensic computer expert made no mention of destroyed or missing files in his report, despite the fact that he analyzed King's Dresser-Rand laptop. More importantly, Dresser-Rand presents no arguments that by deleting files on his laptop, King would have exceeded his authorized access. Dresser-Rand does not point to any restrictions on King's access that, for instance, would allow him to view files on his laptop but forbid him from deleting them. There is therefore insufficient evidence to sustain a CFAA claim against King on this basis.

V. CFAA Claim Against Global Power

Dresser-Rand brings the CFAA claim against all Defendants, including Global Power. Dresser-Rand argues that Global Power is implicated under the CFAA through Jones, King and Wadsworth, working as agents of Global Power. Because the CFAA claim cannot survive against any of these Defendants, it cannot survive against Global Power.

VI. CONCLUSION

For the foregoing reasons I will grant Defendants' partial motion to dismiss the Computer Fraud and Abuse Act claims against all Defendants.

s/Anita B. Brody

____
ANITA B. BRODY, J.

Copies **VIA ECF** on _________ to: Copies **MAILED** on _______ to: